CLAIMS

What is claimed is:

1. A digital signature method comprising the steps of:

generating summary text for an electronic document;

displaying said summary text on the display screen of a terminal of a signatory;

calculating a digest value for said summary text using a function with which a value uniquely representing input data is generated and regeneration of said input data from said value is difficult;

encrypting data, including said digest value, using a private key stored in said terminal, and generating a signature value; and

generating a signed document including said signature value.

2. The digital signature method according to claim 1, wherein said electronic document and said signed document are XML documents, and said summary text is generated using XPath of said electronic document, which is an XML document.

3. The digital signature method according to claim 1, wherein said terminal includes a signature template having a variable field, further comprising the steps of:

adding said digest value to said variable field of said signature template;

employing said function to convert said signature

template to which said digest value has been added; and

employing said private key to encrypt a value obtained by conversion and generating said signature value.

4. The digital signature method according to claim 3, wherein a URI for said electronic document is added to said variable field of said signature template.

5. The digital signature method according to claim 3, wherein said signature template is canonicalized using a predetermined algorithm.

6. The digital signature method according to claim 1, wherein said function is a hash function.

7. A digital signature system comprising:

means for generating summary text for an electronic document;

means for displaying said summary text on the display screen of a terminal of a signatory;

means for calculating a digest value for said summary text using a function with which a value uniquely representing input data is generated and regeneration of said input data from said value is difficult;

means for encrypting data, including said digest value, using a private key stored in said terminal; and

means for generating a signed document including a signature value obtained by the cryptography.

8. The digital signature system according to claim 7, wherein said electronic document and said signed document are XML documents, further comprising:

means for generating said summary text using XPath of said electronic document, which is an XML document.

9. The digital signature system according to claim 7, wherein said terminal includes a signature template having a variable field, further comprising:

means for adding said digest value to said variable field of said signature template;

means for employing said function to convert said signature template to which said digest value has been added; and

means for employing said private key to encrypt a value obtained by conversion.

10. The digital signature system according to claim 9, wherein a URI for said electronic document is added to said variable field of said signature template.

11. The digital signature system according to claim 9, wherein said signature template is canonicalized using a predetermined algorithm.

12. The digital signature system according to claim 7, wherein said function is a hash function.

13. A digital signature method comprising the steps of:

a signature demandant transmitting an electronic

document to an agent;

said agent generating summary text for said electronic document, and transmitting said summary text to a terminal of a signatory;

said signatory displaying said summary text on the display screen of said terminal of said signatory;

said signatory confirming said summary text, and employing a private key stored in said terminal to digitally sign said summary text or a document corresponding to said summary text;

said signatory transmitting, to said agent, a signature value generated by the digital signature;

said agent generating a signed document by adding said signature value to said electronic document; and

said agent transmitting said signed document to said signature demandant.

14. A digital signature system comprising:

means for permitting a signature demandant to transmit an electronic document to an agent;

means for permitting said agent to generate summary text for said electronic document, and to transmit said summary text to a terminal of a signatory;

means for permitting said signatory to display said summary text on the display screen of said terminal of said signatory;

means for permitting said signatory to confirm said summary text, and to employ a private key stored in said terminal to digitally sign said summary text or a document corresponding to said summary text;

means for permitting said signatory to transmit, to said agent, a signature value generated by the digital signature;

means for permitting said agent to generate a signed document by adding said signature value to said electronic document; and

means for permitting said agent to transmit said signed document to said signature demandant.

15. A digital signature mediation method comprising the steps of:

receiving an electronic document from a signature demandant, and generating summary text for said electronic document;

transmitting said summary text to a terminal of a signatory;

generating a signed document by adding, to said electronic document, a signature value received from said terminal of said signatory; and

transmitting said signed document to said signature demandant.

16. The digital signature mediation method according to claim 15, wherein said electronic document and said signed document are XML documents, and said summary text is generated using XPath of said electronic document, which is an XML document.

17. A digital signature mediation system comprising:

means for receiving an electronic document from a

signature demandant, and for generating summary text for said electronic document;

means for transmitting said summary text to a terminal of a signatory;

means for generating a signed document by adding, to said electronic document, a signature value received from said terminal of said signatory; and

means for transmitting said signed document to said signature demandant.

18. The digital signature mediation system according to claim 17, wherein said electronic document and said signed document are XML documents, further comprising:

means for generating said summary text using XPath of said electronic document, which is an XML document.

19. An information terminal comprising:

means for receiving summary text for an electronic document;

means for displaying said summary text on a display screen;

means for calculating a digest value for said summary text using a function with which a value uniquely representing input data is generated and regeneration of said input data from said value is difficult;

storage means for storing a private key;

means for employing said private key to encrypt data, including said digest value; and

means for generating a signature value obtained by the cryptography.

20. The information terminal according to claim 19, further comprising:

storage means for storing a signature template having a variable field;

means for adding, to said variable field of said signature template, said digest value, a URI of said electronic document and other information concerning said electronic document;

means for employing said function to convert said signature template to which said digest value and said information have been added; and

means for employing said private key to encrypt a value obtained by conversion, and generating said signature value.

21. The information terminal according to claim 20, wherein said electronic document is an XML document, and said signature template is canonicalized using a predetermined algorithm.

22. A digital signature method comprising the steps of:

receiving summary text for an electronic document;

displaying said summary text on a display screen;

calculating a digest value for said summary text using a function with which a value uniquely representing input data is generated and regeneration of said input data from said value is difficult;

encrypting data, including said digest value by employing said private key that is recorded in a storage

area of an information terminal, or in a storage area of a memory connectable to said information terminal; and

generating a signature value obtained by the cryptography.

23. The digital signature method according to claim 22, further comprising:

adding said digest value, a URI of said electronic document and other information concerning said electronic document to a variable field of a signature template, which that is recorded in said storage area of said information terminal or in a storage area of a memory connectable to said information terminal;

employing said function to convert said signature template to which said digest value and said information have been added; and

employing said private key to encrypt a value obtained by conversion, and generating said signature value.

24. The digital signature method according to claim 23, wherein said electronic document is an XML document, and said signature template is canonicalized using a predetermined algorithm.

25. A computer-readable storage medium, on which information for a private key, for public key cryptography, and a program are stored that permit a computer to perform:

a function for calculating a digest value for said

summary text using a function with which a value uniquely representing input data is generated and regeneration of said input data from said value is difficult;

a function for employing said private key to encrypt data, including said digest value.

26. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 1.

27. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 13.

28. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing digital signature mediation, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 15.

29. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for a digital signature, said method steps comprising the steps of claim 1.

30. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for a digital signature, said method steps comprising the steps of claim 13.

31. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for a digital signature, said method steps comprising the steps of claim 15.

32. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature system, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 7.

33. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature system, the computer readable program code means in said computer

program product comprising computer readable program code means for causing a computer to effect the functions of claim 14.

34. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature mediation system, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 17.

35. A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing an information terminal, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 19.

37. An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing a digital signature, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 22.

38. A program storage device readable by machine, tangibly embodying a program of instructions executable by

the machine to perform method steps for a digital signature, said method steps comprising the steps of claim 22.